BUSINESS ASSOCIATES

[*45 CFR 164.502(e), 164.504(e), 164.532(d) and (e)*]

Background

By law, the HIPAA Privacy Rule applies only to covered entities – health plans, health care clearinghouses, and certain health care providers. However, most health care providers and health plans do not carry out all of their health care activities and functions by themselves. Instead, they often use the services of a variety of other persons or businesses. The Privacy Rule allows covered providers and health plans to disclose protected health information to these "business associates" if the providers or plans obtain satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule. Covered entities may disclose protected health information to an entity in its role as a business associate *only* to help the covered entity carry out its health care functions – not for the business associate's independent use or purposes, except as needed for the proper management and administration of the business associate.

How the Rule Works

General Provision. The Privacy Rule requires that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity. The satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the covered entity and the business associate.

What Is a "Business Associate?" A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

- A member of the covered entity's workforce is not a business associate.
- A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity.

The Privacy Rule lists some of the functions or activities, as well as the particular services, that make a person or entity a business associate, if the activity or service involves the use or disclosure of protected health information. The types of functions or activities that may make a person or entity a business associate include payment or health care operations activities,

as well as other functions or activities regulated by the Administrative Simplification Rules.

- *Business associate functions and activities include*: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing.

- *Business associate services are*: legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.

See the definition of "business associate" at 45 CFR 160.103.

Examples of Business Associates.

- A third party administrator that assists a health plan with claims processing.

- A CPA firm whose accounting services to a health care provider involve access to protected health information.

- An attorney whose legal services to a health plan involve access to protected health information.

- A consultant that performs utilization reviews for a hospital.

- A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer.

- An independent medical transcriptionist that provides transcription services to a physician.

- A pharmacy benefits manager that manages a health plan's pharmacist network.

Business Associate Contracts. A covered entity's contract or other written arrangement with its business associate must contain the elements specified at 45 CFR 164.504(e). For example, the contract must:

- Describe the permitted and required uses of protected health information by the business associate;

- Provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law; and

- Require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract.

Where a covered entity knows of a material breach or violation by the business associate of the contract or agreement, the covered entity is required to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract or arrangement. If termination of the contract or agreement is not feasible, a covered entity is required to report the problem to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR).

Sample business associate contract language is available on the HHS OCR Privacy of Health Information website at http://www.hhs.gov/ocr/hipaa/contractprov.html.

Transition Provisions for Existing Contracts. Covered entities (other than small health plans) that have an existing contract (or other written agreement) with a business associate prior to October 15, 2002, are permitted to continue to operate under that contract for up to one additional year beyond the April 14, 2003 compliance date, provided that the contract is not renewed or modified prior to April 14, 2003. This transition period applies only to written contracts or other written arrangements. Oral contracts or other arrangements are not eligible for the transition period. Covered entities with contracts that qualify are permitted to continue to operate under those contracts with their business associates until April 14, 2004, or until the contract is renewed or modified, whichever is sooner, regardless of whether the contract meets the Rule's applicable contract requirements at 45 CFR 164.502(e) and 164.504(e). A covered entity must otherwise comply with the Privacy Rule, such as making only permissible disclosures to the business associate and permitting individuals to exercise their rights under the Rule.

See 45 CFR 164.532(d) and (e).

Exceptions to the Business Associate Standard. The Privacy Rule includes the following exceptions to the business associate standard. See 45 CFR 164.502(e). In these situations, a covered entity is not required to have a business associate contract or other written agreement in place before protected health information may be disclosed to the person or entity.

- Disclosures by a covered entity to a health care provider for treatment of the individual.

For example:

- A hospital is not required to have a business associate contract with the specialist to whom it refers a patient and transmits the patient's medical chart for treatment purposes.
- A physician is not required to have a business associate contract with a laboratory as a condition of disclosing protected health information for the treatment of an individual.
- A hospital laboratory is not required to have a business associate contract to disclose protected health information to a reference laboratory for treatment of the individual.

- Disclosures to a health plan sponsor, such as an employer, by a group health plan, or by the health insurance issuer or HMO that provides the health insurance benefits or coverage for the group health plan, provided that the group health plan's documents have been amended to limit the disclosures or one of the exceptions at 45 CFR 164.504(f) have been met.

- The collection and sharing of protected health information by a health plan that is a public benefits program, such as Medicare, and an agency other than the agency administering the health plan, such as the Social Security Administration, that collects protected health information to determine eligibility or enrollment, or determines eligibility or enrollment, for the government program, where the joint activities are authorized by law.

Other Situations in Which a Business Associate Contract Is NOT Required.

- When a health care provider discloses protected health information to a health plan for payment purposes, or when the health care provider simply accepts a discounted rate to participate in the health plan's network. A provider that submits a claim to a health plan and a health plan that assesses and pays the claim are each acting on its own behalf as a covered entity, and not as the "business associate" of the other.

- With persons or organizations (e.g., janitorial service or electrician) whose functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all.

- With a person or organization that acts merely as a conduit for protected health information, for example, the US Postal Service, certain private couriers, and their electronic equivalents.

- Among covered entities who participate in an organized health care arrangement (OHCA) to make disclosures that relate to the joint health care activities of the OHCA.

- Where a group health plan purchases insurance from a health insurance issuer or HMO. The relationship between the group health plan and the health insurance issuer or HMO is defined by the Privacy Rule as an OHCA, with respect to the individuals they jointly serve or have served. Thus, these covered entities are permitted to share protected health information that relates to the joint health care activities of the OHCA.

- Where one covered entity purchases a health plan product or other insurance, for example, reinsurance, from an insurer. Each entity is acting on its own behalf when the covered entity purchases the insurance benefits, and when the covered entity submits a claim to the insurer and the insurer pays the claim.

- To disclose protected health information to a researcher for research purposes, either with patient authorization, pursuant to a waiver under 45 CFR 164.512(i), or as a limited data set pursuant to 45 CFR 164.514(e). Because the researcher is not conducting a function or activity regulated by the Administrative Simplification Rules, such as payment or health care operations, or providing one of the services listed in the definition of "business associate" at 45 CFR 160.103, the researcher is not a business associate of the covered entity, and no business associate agreement is required.

- When a financial institution processes consumer-conducted financial transactions by debit, credit, or other payment card, clears checks, initiates or processes electronic funds transfers, or conducts any other activity that directly facilitates or effects the transfer of funds for payment for health care or health plan premiums. When it conducts these activities, the financial institution is providing its normal banking or other financial transaction services to its customers; it is not performing a function or activity for, or on behalf of, the covered entity.

Frequently Asked Questions

To see Privacy Rule FAQs, click the desired link below:

FAQs on Business Associates

FAQs on ALL Privacy Rule Topics

(You can also go to http://answers.hhs.gov/cgi-bin/hhs.cfg/php/enduser/std_alp.php, then select "Privacy of Health Information/HIPAA" from the Category drop down list and click the Search button.)